Attorney Docket No. 010027

IN THE CLAIMS

Please amend the claims as follows:

1.   (Original)   An authentication apparatus operable to produce a secure identifier, the apparatus comprising:

a processor;

a clock coupled to the processor configurable to generate a time element;

a memory element coupled to the processor configurable to store a private key and public key information;

at least one actuator coupled to the processor;

a signature generator coupled to the processor operable to generate a digital signature, the digital signature being a function of the private key and the time element; and

an emitter coupled to the signal generator operable to emit the secure identifier, the secure identifier comprising the digital signature, time element, and public key information.

2.   (Original)   The apparatus set forth in Claim 1, the signature generator further comprising:

a random number generator coupled to the processor to encrypt the digital signature.

3.   (Original)   The apparatus set forth in Claim 1, wherein the time element comprises a predetermined number of least significant bits of the time.

4.   (Original)   The apparatus set forth in Claim 1, further comprising an input element coupled to the processor, the input element capable of receiving a personal identification number (PIN).

5.   (Original)   The apparatus set forth in Claim 1, further comprising an input element coupled to the processor, the input element capable of receiving a challenge.

6.   (Original)   The apparatus set forth in Claim 1, further comprising a display coupled to the processor, the display capable of displaying key identifiers.

2

(AMENDMENTFORM.VER1.0-07/30/03)

Attorney Docket No. 010027

7.   (Original)   The apparatus set forth in Claim 1, wherein the secure identifier emitted is emitted as an audio tone.

8.   (Original)   The apparatus set forth in Claim 1, wherein the secure identifier emitted is emitted as an optical signal.

9.   (Original)   The apparatus set forth in Claim 1, wherein the actuator is a push-button switch.

10.   (Original)   The apparatus set forth in Claim 1, wherein the actuator is a voice activated switch.

11.   (Original)   The apparatus set forth in Claim 1, wherein the public key information is a public key identifier.

12.   (Original)   The apparatus set forth in Claim 11, wherein the pubic key identifier is derived from the public key information.

13.   (Original)   The apparatus set forth in Claim 1, wherein the public key information is the public key.

14.   (Original)   The apparatus set forth in Claim 1, wherein the digital signature is encrypted using a personal identification number (PIN).

15.   (Original)   A method of authenticating, comprising:
generating a time element;
identifying a key identifier;
generating a digital signature;
generating a secure identifier as a function of the time element, the key identifier, the digital signature; and
emitting the secure identifier.

3

(AMENDMENTFORM.VER1.0-07/30/03)

16.   (Original)   The method set forth in Claim 15, further comprising identifying a PIN, and wherein generating a digital signature is further a function of the PIN.

17.   (Original)   The method set forth in Claim 15, wherein the secure identifier emitted is emitted as an audible tone.

18.   (Original)   The method set forth in Claim 15, wherein the secure identifier emitted is emitted as an optical signal.

19.   (Original)   The method set forth in Claim 15, wherein the digital signature is derived from a private key.

20.   (Original)   An authentication receiver, comprising:
a receiver configurable to receive a secure identifier, the secure identifier comprising:

    a digital signature, the digital signature comprising information derived from a private key,

        a public key identifier; and

        a time identifier; and

    a verifier configurable to verify the secure identifier, the verifier comprising:

        memory comprising information corresponding to the public key information received and time tolerance information;

        a key retriever coupled to the memory and configurable to retrieve a public key corresponding to the public key identifier; and

        a time verifier coupled to the memory and configurable to verify that the received time identifier falls within acceptable time tolerances.

21.   (Original)   The apparatus set forth in Claim 20, the secure identifier further comprises a PIN, and wherein the receiver is configurable to decrypt the digital signature using the PIN.

4

22.   (Original)   The apparatus set forth in Claim 20, wherein the key retriever compares the public key identifier received to public key information stored in memory.

23.   (Original)   The apparatus set forth in Claim 20, wherein the time tolerance information comprises information regarding clock drift.

24.   (Original)   The apparatus set forth in Claim 20, wherein the secure identifier is emitted as an audible tone.

25.   (Original)   The apparatus set forth in Claim 20, wherein the secure identifier is emitted as an optical signal.

26.   (Original)   A method of authenticating, comprising:

receiving a secure identifier, the secure identifier comprising a digital signature, a key identifier, and a time identifier; and

verifying the secure identifier, verifying comprising:

verifying that the public key identifier received corresponds to known information regarding the public key identifier received; and

verifying the time identifier such that the time identifier received is within predetermined time tolerances.

27.   (Original)   The method set forth in Claim 26, the digital signature further comprises a PIN, and where receiving further comprises decrypting at least a portion of the digital signature using the PIN.

28.   (Original)   The method set forth in Claim 26, wherein the secure identifier received is received as an audible tone.

29.   (Original)   The method set forth in Claim 26, wherein the secure identifier received is received as an optical signal.

5

30.   (Cancelled)

31.   (Cancelled)

32.   (Cancelled)

33.   (Cancelled)

34.   (Cancelled)

35.   (Cancelled)

36.   (Cancelled)

37.   (Cancelled)

38.   (Cancelled)

39.   (Cancelled)

40.   (Cancelled)

41.   (Cancelled)

42.   (Cancelled)

43.   (Cancelled)

6

(AMENDMENTFORM.VER1.0-07/30/03)

44.   (Currently Amended) Apparatus for A method of authenticating, comprising:

means for generating a time element;

means for identifying a key identifier;

means for generating a digital signature;

means for generating a secure identifier as a function of the time element, the key identifier, the digital signature; and

means for emitting the secure identifier.

45.   (Currently Amended) The apparatus method set forth in Claim 44, further comprising means for identifying a PIN, and wherein means for generating a digital signature is further a function of the PIN.

46.   (Currently Amended) The apparatus method set forth in Claim 44, wherein the secure identifier emitted is emitted as an audible tone.

47.   (Currently Amended) The apparatus method set forth in Claim 44, wherein the secure identifier emitted is emitted as an optical signal.

48.   (Currently Amended) The apparatus method set forth in Claim 44, wherein the digital signature is derived from a private key.

49.   (Cancelled)

50.   (Cancelled)

51.   (Cancelled)

52.   (Cancelled)

53.   (Cancelled)

7

(AMENDMENTFORM.VER1.0-07/30/03)

54.   (Cancelled)

55.   (Currently Amended) Apparatus for A method of authenticating, comprising:
means for receiving a secure identifier, the secure identifier comprising a digital signature, a key identifier, and a time identifier; and

means for verifying the secure identifier, verifying comprising:

means for verifying that the public key identifier received corresponds to known information regarding the public key identifier received; and

means for verifying the time identifier such that the time identifier received is within predetermined time tolerances.

56.   (Currently Amended) The apparatus method set forth in Claim 55, the digital signature further comprises a PIN, and where means for receiving further comprises decrypting the digital signature using the PIN.

57.   (Currently Amended) The apparatus method set forth in Claim 55, wherein the secure identifier received is received as an audible tone.

58.   (Currently Amended) The apparatus method set forth in Claim 55, wherein the secure identifier received is received as an optical signal.

8